DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 2: Gateways

1. References.

a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

d. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

e. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

f. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

g. USASC Memorandum, "Top Level Architecture (TLA) Implementation Guide", 25 September 2000.

h. USANETA TR #DSED00042, "TLA 7204VXR/7206VXR and 2900 XL Series Switch Implementation Guide", 16 August 2000.

i. 4ID Policy # 5: Passwords, 22 March 2007.

2. Purpose:

a. Application-level gateways allow the network administrator to implement a much stricter security policy than with a packet-filtering router. Special purpose code (a proxy service) is installed on the gateway (or gateways) for each desired application. If the network administrator does not install the proxy code for a particular application, the service is not supported and cannot be forwarded across the gateway. Also, the proxy code can be configured to support only those specific features of an application that the network administrator considers acceptable while denying all other features.

b. Because gateways interleave protected and public networks they present inherent IA risks to owners and users of protected IT resources. This policy provides the framework for implementing consistent networking and gateway solutions throughout the Network.

3. Applicability. This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. 4ID G6 will ensure that appropriate application and circuit level gateway security policies are established.

b. Information Assurance Manager (IAM) will:

(1) Ensures the gateway policy is written that describes the intended functionality of the gateway and that the gateway as installed enforces that policy.

(2) Ensures that the gateway administrator (SA) receives training to operate the gateway.

c. Information Assurance Security Officer (IASO) will:

(1) Ensure the certification and accreditation is completed and current on the gateway installation.

(2) Ensure that the gateway is operated and maintained according to the vendor's specifications and organizational requirements.

(3) Working with the gateway administrator, ensure that the gateway audit log is reviewed frequently.

(4) Report any security incidents involving the gateway as required by the organizational security regulations, and to the IAM.

(5) Ensure the gateway security policy is implemented and carried out properly. Continuously evaluate the gateway security environment. Make recommendations to the IAPM as appropriate.

d. Gateway Administrator will:

(1) Understand and monitor the configuration of the gateway.

(2) Each gateway shall be configured with user ID and password access controls that are compliant with the 4ID password policy.

(3) Ensure that the gateway is continuously afforded effective physical security.

(4) Make frequent backups of data and files on the gateway and ensure that gateway software integrity is maintained.

(5) Respond to any alarms or alerts from the gateway software as quickly as possible.

(6) In coordination with the IASO, ensure adequate security is maintained over the gateway.

(7) Install IAVA patches and corrective patches to the gateway software as required.

(8) Review the audit logs on the gateway on a daily basis.

(9) Report any attacks or incidents on the gateway to the gateway IASO.

5. Policy:

a. Network (and Gateway) Requirements Analysis and Planning

(1) Requirement analyses shall precede deployment of application-level gateways (proxy servers). User organization and system owner personnel shall communicate their requirements to a designated 4ID service provider organization, which shall be signed-off

and approved by appropriate user-organization decision authorities. Minimum functional requirements and planning subjects include:

(a) Organization size (i.e., number of segments and nodes)

(b) Specific connectivity permissions.

(c) Specific connectivity prohibitions.

(d) Information security requirements.

(e) Bandwidth requirements.

(f) Protocol and Port requirements

(g) Load balancing, alternate routing, and survivability requirements.

(2) Network design, deployment of application-level gateway devices, and connectivity routing paths shall be implemented (configured, tested, validated, and documented) as required to satisfy transport, connectivity, and security requirements.

(3) Application-level gateways and related networking devices shall be configured in concert with gateway and other IA safeguards to meet user (or IT system) defined security requirements and traffic volumes.

(4) Initial configurations shall establish configuration management baselines on user organization – routing element basis. Required configurations shall be thoroughly tested, validated, and documented before placing new routing, networking, (gateway proxy devices) or configuration modifications into production.

b. Gateway Configuration Management, Testing, Validation, and Documentation:

(1) Application-level Gateway architecture and capacity planning shall be included in annual Information Resource Management (IRM) service delivery and MOA reviews.

(2) New software releases, configuration updates, and access or routing modifications shall be documented, tested, validated, approved by the Configuration Control Board (CCB) and added to configuration management records prior to deployment.

c. Operation and Maintenance:

(1) Application-level Gateway Device Controls - - to be implemented when applicable.

(a) Individual administrators and technicians who access, repair, and modify gateway configurations shall be specifically identified.

(b) Individuals accessing gateway devices are required to enter a user ID and password. User profiles shall govern the access rights of the user.

(c) Guest accounts shall be disabled.

(d) Administrator accounts shall be renamed.

(e) The use of shared group ID's will not be allowed. However, the use of Group memberships, where users maintain individual user ID's and the Group membership controls rights and permissions for the group, is permissible.

(f) Remote administration of gateways over the NIPRNet, Internet, etc., shall be accomplished via a secure communications path (e.g., VPN, etc.).

(2) Accountability: Audit information shall be retained and protected so that actions affecting security can be traced to the responsible party.

(3) Continuous Protection:

(a) Data from "protected" mechanisms that document application-level gateway device system administration, rule set modifications, operation, and performance shall be continuously protected against tampering and/or editing.

(b) Attempts to modify system services, whether successful or not, shall be recorded and retained in security logs.

(c) Security, application, and system audit logs shall be copied nightly. Systems shall be backed up on a regular basis and stored in secure directories. Additional tape backup copies of system files shall be created and readily available for use by IA staff.

(4) Physical Security: Gateway devices shall be located in secured facilities with controlled access. Individuals not on the access list will sign in and be under continuous escort.

(5) Documentation and Configuration Management:

(a) Maintenance of up-to-date gateway configuration documentation and change management records is the responsibility of 4ID service providers who implement and technically support networking and routing requirements of respective end-user organizations.

(b) Changes to the configuration baseline shall be in accordance with the 4ID Configuration Management Plan (CMP) and coordinated and/or approved by the 4ID Configuration Control Board (CCB).

6. Compliancy Checks: Each Gateway device shall be scanned at least twice a year using approved security scanning software. If any of the gateway devices are found to be non-compliant with the above policy, corrective actions will be taken to correct deficiencies.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding